Step 520 - Store the new key to a memory.

Step 530 - Split the pair (Stop copying data to remote disk system).

Step 540 - Split the pair.

Step 550 - Store the new key to Key210 to validate it.

Step 560 - Store the new key to Key210 to validate it.

Step 570 - Re-synchronize the pair (start copying data to the remote disk system).

Step 580 - Re-synchronize the pair. --

Please add the following new paragraph ~~at~~ before line 8, before the second paragraph, on page 8: JH 3/14/07

-- The encryption and decryption techniques of Fig. 6 are summarized as follows:

Step 610 - Store "encryption = NO and decryption = NO" to a memory and send it to the remote disk system.

Step 620 - Store "encryption = NO and decryption = NO" to a memory.

Step 630 - Get the current I/O number of the volume pair.

Step 640 - Choose the appropriate I/O number (the boundary number) to switch encryption and decryption off and send it to remote disk system.

Step 650 - Wait for the I/Os with the boundary number; I/Os with the boundary number or smaller are decrypted with the current key.

Step 660 - Wait for the I/Os with the boundary number; I/Os with the boundary number or smaller are encrypted with the current key.

Step 670 - Store "NO" to Encryption220 and Decryption230; I/Os with the number greater than the boundary number are not encrypted.

Step 680 - Store "NO" to Encryption220 and Decryption230; I/Os w/the number greater than the boundary number are not decrypted. --

Please add the following new paragraph after the above paragraph and before the second paragraph, on page 8:

-- The encryption and decryption techniques of Fig. 7 are summarized as follows:

Step 710 - Store "encryption = NO and decryption = NO" to a memory and send it to the remote disk system.

Step 720 - Store "encryption = NO and decryption = NO" to a memory.

Step 730 - Split the pair (Stop copying data to remote disk system).

Step 740 - Split the pair.

Step 750 - Store "NO" to Encryption220 and Decryption230.

Step 760 - Store "NO" to Encryption220 and Decryption230.

Step 770 - Re-synchronize the pair (start copying data to the remote disk system).

Step 780 - Re-synchronize the pair. --

before JJ 3/14/07

Please add the following new paragraph after the above paragraph ~~at~~ line 30, after the third paragraph, on page 8:

-- The transparent key exchange technique of Fig. 8 is summarized as follows:

Step 800 - Set all bits of the re-encryption bitmap to 1 (one).

Step 810 - Copy request exists from the local disk system? If yes, go to Step 890. If no, proceed to step 820.

the write at the remote disk is complete, a message 350 is sent to the local disk system, informing it of the completion. --

YJ 3/14/07

Please add the following new paragraph ~~at~~ before line 10, after the second paragraph, on page 7:

-- Accordingly, the first method of transparent key exchange is summarized as follows:

Step 410 - Store a new key to a memory and send it to the remote disk system.

Step 420 - Store the new key to a memory.

Step 430 - Get the current I/O number of the volume pair.

Step 440 - Choose the appropriate I/O number (the boundary number) to validate the new key and send it to remote disk system.

Step 450 - Wait for the I/Os with the boundary number; I/Os with the boundary number or smaller are decrypted with the current key.

Step 460 - Wait for the I/Os with the boundary number; I/Os with the boundary number or smaller are encrypted with the current key.

Step 470 - Set the new key to Key210; I/Os with the number greater than the boundary number are encrypted with the new key.

Step 480 - Set the new key to Key210; I/Os with the number greater than the boundary number are decrypted with the new key. --

YJ 3/14/07

Please add the following new paragraph ~~at~~ before line 1, before the first paragraph, on page 8:

-- Accordingly, the second method of implementing key exchange is summarized as follows:

Step 510 - Store a new key to a memory and send it to the remote disk system.